IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

1. (currently amended) An information processing method for calculating x*(2^n) mod P for an input value x larger than a prime number P, the operator ^ denoting power, without directly obtaining x*(2^n) mod P of the input value x divided by P, thereby making the estimation of P difficult in a tamper resistant storage device, said tamper resistant storage device includes an information processing apparatus, said information processing method being executed by said ~~an~~ information processing apparatus which includes ~~comprising~~ a ~~first~~ memory being of at least n bits sufficient for storing the modulus P, ~~a second memory~~ also being of at least m bits sufficient for storing said input value x~~,~~ and ~~a third memory for~~ storing 2^(2m+n) mod P, and a Montgomery modular multiplication device, said information processing method, being executed by said information processing apparatus, comprising the steps of:

storing said input value x in said ~~first~~ memory ~~of n bits~~;

calculating 2^(2m+n) mod P or reading said 2^(2m+n) mod P from said ~~third~~ memory by said Montgomery modular multiplication device;

reading said input value x from said ~~first~~ memory ~~of n bits~~;

calculating x1 = x*2^(2m+n)*(2^(-m)) mod P = x*2^(m+n) mod P by said Montgomery modular multiplication device;

calculating x2 = x1*(2^(-m)) mod P = x*(2^n) mod P to transfer said input value x into x*(2^n) mod P without explicitly obtaining x mod P; and

storing said transferred value.

2. (currently amended) An information processing method for calculating x*(2^n) mod P for an input value x larger than a prime number P, the operator ^ denoting power, without directly obtaining x*(2^n) mod P of the input value x divided by P, thereby making the estimation of P difficult in a tamper resistant storage device, said tamper resistant storage device includes an information processing apparatus, said information processing method being executed by said ~~an~~ information processing apparatus which includes ~~comprising~~ a ~~first~~ memory being of at least n bits sufficient for storing the modulus ~~modules~~ P, also being ~~a second memory~~ of at least m bits sufficient for storing said input value x~~,~~ a ~~third memory for~~ storing 2^(m+2n) mod P and a Montgomery modular multiplication device, said information processing method, being executed by said information processing apparatus, comprising the steps of:

storing said input value x in said ~~first~~ memory ~~of n bits~~;

calculating 2^(m+2n) mod P or reading said 2^(m+2n) mod P from said ~~third~~ memory by said Montgomery modular multiplication device;

reading said input value x from said ~~sadi first~~ memory ~~of n bits~~;

calculating x1 = x*2^(m+2n)*(2^(-m)) mod P = x*2^(2n) mod P by said Montgomery modular multiplication device; and

calculating x2 = x1*(2^(-n)) mod P = x*(2^n) mod P to transfer said input value x into x*(2^n) mod P without explicitly obtaining x mod P; and

storing said transferred value.

Claim 3 (canceled).

4. (currently amended) The information processing method of claim 1, for an RSA cryptosystem method using Chinese Remainder Theorem, said method comprising the steps of:

calculating mod P using the information processing method according to claim 1 and encrypting said input value x; and

storing said encrypted input value x.

5. (currently amended) The information processing method of claim 2, for an RSA cryptosystem method using Chinese Remainder Theorem, said method further comprising the steps of:

calculating mod P using the information processing method according to claim 2, and encrypting said input value x; and

storing said encrypted input value x.

6. (currently amended) An information processing apparatus, included in a tamper resistant storage device, for calculating x*(2^n)mod P for an input value x larger than a prime number P, the operator ^ denoting power, without directly obtaining x*(2^n) mod P of the input value x divided by P, thereby making the estimation of P difficult in said tamper resistant storage device, said information processing apparatus comprising:

a memory of at least n bits sufficient for storing the modulus P;

wherein said ~~a~~ memory being also of at least m bits sufficient for storing said input value x, and

a Montgomery modular multiplication device, wherein said Montgomery modular multiplication device adapted to execute the steps of

calculating 2^(2m+n) mod P;

reading said input value x from said memory ~~of n bits~~; and

calculating x1=x*2^(2m+n)*(2^(-m)) mod P=x*2^(m+n) mod P and – x2=x1*(2^(-m)) mod P = x*(2^n) mod P to transfer said input value x into x*(2^n) mod P without explicitly obtaining x mod P.